REMARKS

Claims 1-21 are pending in the instant application and stand rejected by the examiner. Claims 1 and 11 are independent claims. Reconsideration is respectfully requested in light of the amendments and remarks contained herein.

Claim Rejections – 35 U.S.C. §§ 102, 103

Claims 1-21 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over the combination of Audebert (U.S. Patent Pub. No. 2003/0005317) in view of Paatero (U.S. Patent Pub. No. 2003/0163685).

While assignee disagrees with the current rejections, independent claims 1 and 11 have been amendment to further define over the cited references. It is respectfully submitted that the combination of Audebert and Paatero does not teach a domain controller configured to control a plurality of domains on a mobile device for controlling access to the different types of assets that require a common level of trust to access within a domain. The outstanding office action correctly admits that Audebert does not disclose a domain controller at page 4, line 10.[1]

It is respectfully submitted that Paatero does not contain any teaching of multiple domains at all let alone domains that contain assets requiring a common level of trust to access. Thus, it is not possible for Paatero to teach a domain controller, configured to control the plurality of domains on the mobile device, for controlling access to the different types of assets that require a common level of trust to access within a domain. Paatero describes a system where a role certificate is received from a certificate authority (CA) that contains permitted

[1] It is also noted that the office action correctly admits that the domains of Audebert are very different than the claimed domains. *See* office action at page 4, lines 9-10 stating, "Audebert does not expressly disclose the different types of assets within a domain requiring a common level of trust to access." The Audebert domains allow different applications to store keys and certificates on a device. However, Audebert, like Paatero, does not at all disclose any concept of a common level of trust being required to access assets within a domain.

activities for an identified third party. *See* Paatero, FIG. 2 at 30. This process is further described at paragraphs [0032]-[0033] of Paatero, which state:

> [0032]...If a match is found, then the parsed activity in step 38 is permitted with respect to the identified third parties. This is shown in step 44. Otherwise, no permitted activities are allowed with respect to the non-identified third parties (see step 46).
> [0033] With respect to identifying third parties in the role certificate, this can be done by storing a public key of the third party in the certificate and later determining if the received public key from the third party matches that within the certificate. The storing of the third party public key can preferably be done by storing a hash of the third party public key and then performing a hash of the received public key from the third party (using the same algorithm as used to store the hash value of the third party public key in the certificate) so as to determine if the two hashes are identical. If they are, then the identity of the third party is assumed to be correct.

Thus, a role certificate identifies actions that are permitted to be performed on the device. However, there is no concept of a plurality of domains having assets that require a common level of trust to access. Without domains, it is impossible for Paatero to teach the domain controller, configured to control the plurality of domains on the mobile device, for controlling access to the different types of assets that require a common level of trust to access. Because the combination of references does not teach the domain controller recited in the amended independent claims, it is respectfully requested that the § 103 rejections of claims 1 and 11 be withdrawn.

Assignee also disagrees with certain other rejections of the current office action. For example, claim 3 requires that the domain controller determines whether an entity has a trust relationship with a domain based on whether the entity is within the same domain as the asset the entity is seeking to affect. As described throughout the application at issue, including at paragraph [0106], in some configurations, each member of a domain is trusted and has access to assets within that domain. In rejecting claim 3, the office action cites to FIG. 2 of Paatero and paragraphs [0031]-[0032]. As discussed above, these portions of Paatero describe receiving role

certificates that describe actions that can be performed by different entities. There is no determination of whether an entity seeking to affect an asset and the asset sought to be affected are within the same domain. Because the combination of Audebert and Paatero does not teach this feature, it is respectfully requested that the § 103 rejection of claim 3 be withdrawn.

Arguments have not been provided at this time in support of the patentability of certain of the dependent claims. It is respectfully submitted that because the independent claims are now in condition for allowance, the dependent claims which depend directly or indirectly therefrom are also in condition for allowance. However, assignee reserves the right to argue the patentability of certain of the dependent claims in the instant application at a future time, should that become necessary.

CONCLUSION

For the foregoing reasons, the assignee respectfully submits that the pending claims are allowable. Therefore, the assignee respectfully requests that the examiner pass this case to issuance.

Respectfully submitted,

December 30, 2009

By: Matthew W. Johnson

Matthew W. Johnson
Reg. No. 59,108
Jones Day
North Point; 901 Lakeside Avenue
Cleveland, OH 44114
(412) 394-9524